Wilson & Brown, PLLC
2066 Central Park Avenue
Yonkers, New York 10710
Telephone: (646) 498-9816
Facsimile: (718) 425-0573
Karen N. Wilson-Robinson, Esq.
karen@wilsonbrownlawyers.com

Casey Gerry Schenk
Francavilla Blatt & Penfield, LLP
110 Laurel Street
San Diego, California 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
Gayle M. Blatt, Esq., *pro hac vice application forthcoming*
gmb@cglaw.com

Counsel for Plaintiffs and the Class

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW JERSEY

RICARDO VILLALOBOS AND JEREMY ADAMS, individually, and on behalf of all others similarly situated, *Plaintiffs*, v. VOLKSWAGEN GROUP OF AMERICA, INC., AUDI OF AMERICA, LLC, and SANCTUS, LLC d/b/a SHIFT DIGITAL, *Defendants*.	Case No. 2:21-cv-13049-JMV-JBC Civil Action **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Ricardo Villalobos and Jeremy Adams ("Plaintiffs"), who can be reached through their attorney Karen N. Wilson-Robinson at 2066 Central Park Avenue, Yonkers, New York 10710 on behalf of themselves and all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, allege the following against Defendants Volkswagen Group of America, Inc., ("VGoA") Audi of America, LLC ("Audi"), and Sanctus, LLC d/b/a Shift Digital ("Shift Digital") (collectively, "Defendants").

NATURE OF THE CASE

1. In a recent Executive Order, President Joe Biden reaffirmed that "[t]he United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." *Id*. Among other things, the Order noted that "[t]he private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust

we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced." *Id*.

2. Here, unfortunately, Defendants VWoA, Audi, and Shift Digital violated that trust, leaving Plaintiffs and the putative Class to incur the consequences. As a result, 3.3 million persons had their sensitive personal identifying information ("PII") stolen from Defendants by computer hackers in a cyber-attack (the "Data Breach"). The information stolen in the Data Breach includes name, mailing address, email address, phone number, information about a vehicle purchased, leased, or inquired about including the Vehicle Identification Number ("VIN"), make, model, year, color, and trim and, in some instances, buyers' or interested parties' driver's license numbers, Social Security numbers, account or loan numbers, and tax identification numbers.

3. Plaintiffs Villalobos and Adams bring this class action lawsuit on behalf of a Nationwide Class and Florida and California Sub-Classes (together, the "Classes") to address Defendants' inadequate safeguarding of class members' PII.

4. Armed with the PII accessed in the Data Breach, data thieves can commit numerous crimes including opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medicalservices, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' information, obtaining driver's licenses in Class members' names butwith another person's photograph, and giving false information to police during an arrest.

5. Indeed, new outlets are already reporting that the information stolen in the Data Breach is being sold on well-known hacking forums. *See, e.g.*, Lorenzo Fracheschi-Bicchierai, *Hackers Are Selling Data Stolen From Audi and Volkswagen*, VICE (June 17, 2021, 6:00 a.m.), https://www.vice.com/en/article/xgxaq4/hackers-are-selling-data-stolen-from-audi-and-volkswagen; Lawrence Abrams, *Audi, Volkswagen customer data being sold on hacking forum*, BLEEPING COMPUTER (June 17, 2021, 2:48 pm), https://www.bleepingcomputer.com/news/security/audi-volkswagen-customer-data-being-sold-on-a-hacking-forum/. This

shows the clear value of the stolen data to identity thieves and the imminent peril faced by Plaintiffs and the members of the Class.

6. A recent memo to VGoA dealers obtained by automotive journalism website Automotive News reveals that the vendor involved in the Data Breach is Michigan-based Shift Digital. The information obtained in the Data Breach was contained in a file that Shift Digital left unsecured[1].

7. As a result of the Data Breach, Plaintiffs and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now, and in the future, closely monitor their financial accounts to guard against identity theft.

8. Plaintiffs and Class members will also incur out of pocket costs for things such as paying for credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

---

[1] David Shepardson, *VW says data breach at vendor impacted 3.3 million people in North America*, YAHOO! FINANCE (June 11, 2021), https://finance.yahoo.com/news/vw-says-data-breach-vendor-162407216.html

9. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals whose PII was accessed during the Data Breach.

10. Plaintiffs and the Class request remedies including damages, reimbursement of out-of-pocket costs, and equitable and injunctive relief, including improvements to Defendants' data security systems, future annual audits, and ID protection services funded by Defendants.

PARTIES

11. Plaintiff Ricardo Villalobos is resident of the state of California. He has owned or leased three Audi vehicles since 2017. According to Audi, his PII was compromised in the Data Breach.

12. Plaintiff Jeremy Adams is a resident of the State of South Carolina. He purchased an Audi in Florida in 2017. According to Audi, his PII was compromised in the Data Breach.

13. Defendant Volkswagen Group of America, Inc. is a corporation incorporated in New Jersey with its principal place of business in Herndon, Virginia. Defendant VWoA is the North

American subsidiary of Volkswagen AG.

14. Defendant Audi of America, LLC is a registered trade name of VWoA and has its principal place of business in Herndon, Virginia.

15. Defendant Sanctus, LLC d/b/a Shift Digital is a limited liability company headquartered in Birmingham, Michigan. Shift Digital claims to have invented "digital marketing program optimization" and its website touts its "data omniscience." At the time of the Data Breach, Shift Digital worked with Defendants VWoA and Audi on marketing.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the class are citizens of states different from Defendants.

17. This Court has personal jurisdiction over Defendants

because Defendants conduct business in and throughout New Jersey, and the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) because Defendant VWoA is incorporated in this District and all defendants regularly transact business here. Further, venue is proper under 28 U.S.C. § 1391(b)(3) because all Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

19. Defendant VWoA is the North American subsidiary of Volkswagen AG, a German-based manufacturer of cars and other vehicles worldwide. Audi is a trademark of VWoA and a well-known brand of luxury cars. Shift Digital provides VWoA and Audi with marketing tools, data management, and other functions.

20. Collectively, Defendants sell and market Volkswagen

and Audi cars and trucks in the United States. As a part of that process, they collect various types of PII from customers and potential customers, including name, mailing address, email address, phone number, and information about a vehicle purchased, leased, or inquired about including the Vehicle Identification Number ("VIN"), make, model, year, color, and trim. In the event the buyer or potential buyer purchases the vehicle or applies to Defendants for financing, Defendants also collect the buyers' or interested parties' driver's license numbers, Social Security numbers, account or loan numbers, and tax identification numbers.

21. From 2014 through 2019, Defendants collected the PII of approximately 3.3 million North American customers. It is reported that roughly 90,000 of those customers' driver's license numbers, Social Security numbers, account or loan numbers, or tax identification numbers were exposed in the Data Breach. Defendants VWoA and Audi reported that PII of the remaining Class members was also compromised in the Data Breach.

22. While Defendants are more than happy to monetize that information, and despite the very sensitive nature of that information

and the clear potential for misuse, Defendants left that data stored unsecured for *two years*.

23. In early March 2021, Defendants were informed that unauthorized third parties had gained access to this PII. Following an investigation, in May 2021, Defendants confirmed the PII was left unsecured and that it had been stolen by cyberthieves.

24. In June 2021, Defendants VWoA and Audi began notifying affected customers and state attorneys general about the breach and data theft. On information and belief, Defendant Shift Digital has not provided any notices to affected Class Members.

25. Just a few days later, the information stolen in the Data Breach showed up for sale on well-known hacking forums. *See, e.g.*, Lorenzo Fracheschi-Bicchierai, *Hackers Are Selling Data Stolen From Audi and Volkswagen*, VICE (June 17, 2021, 6:00 a.m.), https://www.vice.com/en/article/xgxaq4/hackers-are-selling-data-stolen-from-audi-and-volkswagen; Lawrence Abrams, *Audi, Volkswagen customer data being sold on hacking forum*, BLEEPING COMPUTER (June 17, 2021, 2:48 pm), https://www.bleepingcomputer.com/news/security/audi-

volkswagen-customer-data-being-sold-on-a-hacking-forum/.

26. Plaintiff Ricardo Villalobos has leased three Audi vehicles since 2017 from Audi Pacific located in Torrance, California; Walter's Audi located in Riverside, California; and Audi Pasadena, located in Pasadena, California.

27. Plaintiff Villalobos provided his PII to Defendants to lease his Audi vehicles with the understanding that it would be protected, maintained, and safeguarded from unauthorized users or disclosure, and that he would be timely notified of any unauthorized disclosure of his PII. He would not have agreed to provide his PII to Defendant, or would have taken precautions to protect it had he known that Defendant would not safeguard it.

28. Plaintiff Villalobos received a letter from Audi of America, dated June 11, 2021, informing him that his information was affected by the Data Breach. A code contained in the letter indicates that he was one of the victims who had the full panoply of PII stolen, including potentially his driver's license number, Social Security number, account numbers, and tax identification number.

29. The letter from Defendant Audi instructed Mr. Villalobos

to, among other things, "look out for spam emails" and "[b]e cautious when opening links or attachments from unsolicited third parties." It also provided him an option to enroll in credit monitoring and identity theft recovery services.

30. After receipt of the Notice letter, Plaintiff Villalobos made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach and reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time he otherwise would have spent on other activities.

31. Plaintiff Villalobos suffered additional actual injury from having his PII compromised in the Data Breach including: (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft and fraud.

32. Plaintiff Adams purchased an Audi in Tampa, Florida in 2017 from Reeves Import Motorcars.

33. Plaintiff provided his PII to Defendants to purchase his

Audi vehicle with the understanding that it would be protected, maintained, and safeguarded from unauthorized users or disclosure, and that he would be timely notified of any unauthorized disclosure of his PII. He would not have agreed to provide his PII to Defendants, or would have taken precautions to protect it had he known that Defendants would not safeguard it.

34. Plaintiff Adams received an email from Audi of America, dated June 20, 2021, informing him that his information was affected by the Data Breach.

35. The email from Defendant Audi instructed Mr. Adams to, among other things, "look out for spam emails" and "[b]e cautious when opening links or attachments from unsolicited third parties."

36. Following the Data Breach, in April 2021, Adams' information was fraudulently used to apply for a line of credit.

37. In July 2021, Adams received a letter from Chase Bank saying that they declined an application because they were concerned that someone may be using his information fraudulently.

38. After receipt of the Notice letter, Plaintiff Adams made reasonable efforts to mitigate further impact of the Data Breach. He

spent time researching the Data Breach and reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time he otherwise would have spent on other activities.

39. Plaintiff Adams suffered additional actual injury from having his PII compromised in the Data Breach including: (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft and fraud.

A. The PII exposed by Defendants is very valuable to identity thieves

40. The information exposed by Defendants is a very valuable to phishers, hackers, identity thieves and cyber criminals, especially at this time where unprecedented numbers of fraudsters are filing fraudulent unemployment benefit claims.

41. Cybercrime has been on the rise for the past decade and continues to climb exponentially; as of 2013 it was being reported that nearly one out of four data breach notification recipients become a

victim of identity fraud.[2]

42. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. This is because malicious actors buy and sell that information for profit.[3] And, indeed, it appears this is already happening with the PII stolen in the Data Breach here.

43. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

44. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PI] belonging to victims from countries all over the world. One

[2] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[3] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May. 29, 2021).

of the key challenges of protecting PI online is its pervasiveness. As data disclosures in the news continue to show, PI about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[4]

45. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[5]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[6]. Criminals can also purchase access to entire company data breaches from $900 to $4,500[7].

---

[4] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited May 29, 2021).

[5] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited May 29, 2021).

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 29, 2021).

[7] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited May 29, 2021).

46. Social Security numbers are among the worst kind of personal information to have stolen because they can be misused so many different ways and are very hard to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[8]

47. And it is no easy task to change or cancel a stolen Social Security number. Plaintiffs and the Class members cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend

[8] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 21, 2021).

against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

49. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[10]

---

[9] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

[10] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, (April 20, 2021), *available at*: https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last visited May 29, 2021).

50. National credit reporting company Experian blogger Sue Poremba also emphasized the value of driver's license to thieves and cautioned:

> If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license is one of the most important pieces to keep safe from thieves.[11]

51. In fact, according to CPO Magazine, which specializes in news, insights and resources for data protection, privacy, and cyber security professionals, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: "It's a gold mine for hackers. With a driver's license number, bad actors can

[11] Sue Poremba, *What should I do If My Driver's License Number is Stolen?* (Oct. 24, 2018), *available at*: https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited May 29, 2021).

manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email."

52. Drivers' license numbers have been taken from auto-insurance providers by hackers in other circumstances, indicating both that this particular form of PII is in high demand and also that Defendants knew or had reason to know that safeguarding their customers' data was of particular importance[12].

[12] *See* United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (accessed Apr. 27, 2021) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021) (describing a scam involving drivers' license numbers and

53. The data stolen in this case commands a high price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[13]

54. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

55. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

56. Victims of drivers' license number theft also often suffer

---

Progressive Insurance).

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

B. Defendants failed to comply with Federal Trade Commission requirements for data security

57. Federal and State governments have established security standards and issued recommendations to minimize data disclosures and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[15]

[14] *See* Federal Trade Commission, *Start With Security* (June 2015), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 29, 2021).

[15] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 29, 2021).

Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[16]

59. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[17]

60. Highlighting the importance of protecting against data disclosures, the FTC has brought enforcement actions against

[16] *Id.*

[17] Federal Trade Commission, *Start With Security*, *supra* footnote 25.

businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[18]

61. Through their negligence in failing to secure Plaintiffs' and Class Members' PII, and in failing to encrypt it, Defendants failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and the Class Members' PII. Defendants' inadequate data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, in addition to violation of the Drivers' Privacy Protection Act, 18 U.S.C. § 2724 ("DPPA").

C. Plaintiffs and the Class members suffered damages as a result of Defendants' failure to protect their PII

[18] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 8, 2021).

62. Plaintiffs and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

63. The ramifications of Defendants' failure to keep individuals' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[19]

64. The PII belonging to Plaintiffs and Class Members is private, sensitive in nature. Defendants failed to obtain Plaintiffs' and Class members' consent to disclose such PII to any other person as required by applicable law and industry standards.

65. Defendants' inattention to the possibility that anyone could obtain the PII of any customer or potential customer of Defendants left Plaintiffs and Class members with no ability to protect their sensitive and private information.

66. Defendants had the resources necessary to prevent the Data Disclosure, but neglected to adequately implement data security

[19] *2014 LexisNexis True Cost of Fraud Study*, (August 2014), *available at*: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited May 29, 2021).

measures, despite its obligations to protect PII of the Plaintiffs and Class members from unauthorized disclosure.

67. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they could have prevented the intrusions into their systems and, ultimately, the theft of PII.

68. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have been placed at an immediate and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family to mitigate the actual and potential impact of the Data Breach on their lives.

69. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take

more than a year for some victims."[20]

70. As a result of Defendants' failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

[20] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited May 29, 2021).

d. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

f. Emotional distress, anguish, and worry about their PII being sold on the dark web, being in the possession of malicious actors, and being misused.

71. In addition to a remedy for the above harms, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft. Plaintiffs therefore request the injunctive remedies outlined in the Prayer of this Complaint.

72. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of the following national class ("Nationwide Class"):

> All persons residing in the United States whose PII, as defined herein, was compromised in the Data Breach that Defendants announced in June 2021.

73. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of the following California state subclass ("California Subclass"):

> All persons residing in the State of California whose PII, as defined herein, was compromised in the Data Breach that Defendants announced in June 2021.

74. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of the following Florida state subclass ("Florida Subclass"):

> All persons residing in the State of Florida whose PII, as defined herein, was compromised in the Data Breach that Defendants announced in June 2021.

75. The Nationwide Class and state subclasses are collectively referred to herein as "Class" unless otherwise stated.

76. Excluded from the proposed Class are the Defendants, including their corporate affiliates and any entities in which they have a controlling interest or that are controlled by Defendant, as well as the

officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants.

77. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division, or create and seek certification of additional classes, after having had an opportunity to conduct discovery.

Numerosity

78. Although the exact number of Class members is uncertain, Defendants have reported it to be around 3.3 million people. This number is clearly great enough that joinder is impracticable. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and to the Court. The Class members may be identified by objective means, such as through information and records in Defendants' possession, custody, or control.

Commonality and Predominance

79. Common questions of law and fact exist as to the proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants' data security measures to protect Plaintiffs' and Class member's PII were reasonable in light of industry standards, the sensitivity of the information involved, the FTC data security recommendations, applicable cybersecurity standards, and best practices recommended by data security experts;

c. Whether Defendants violated the various state laws identified herein;

d. Whether Defendants' failure to implement adequate data security measures resulted in or was the proximate cause of the Data Breach;

e. Whether Defendants' conduct, including their failure to act, was a legal cause of the loss of PII of Plaintiffs and Class members;

f. Whether Defendants owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, and safeguarding their PII;

g. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

h. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

i. Whether Plaintiffs and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

Typicality

80. Plaintiffs' claims are typical of the claims of the Class members. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties.

Adequacy of Representation

81. Plaintiffs are adequate representative of the Class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will

prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

Superiority

82. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT 1

Negligence

(On behalf of the Nationwide Class and all Subclasses)

(As to all Defendants)

83. Plaintiffs incorporate by reference all allegations in paragraphs 1 through 82 as though fully set forth herein.

84. Plaintiffs bring this claim against Defendants VWoA, Audi America, and Shift Digital on behalf of themselves, the National Class, and the Florida and California Subclasses.

85. Defendants owe a duty to Plaintiffs and the Class to exercise reasonable care in securing, safeguarding, storing, and protecting Plaintiffs' and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing their data security systems to ensure that Plaintiffs' and Class members' PII in Defendants' possession was and is adequately secured and protected. Defendants also owe a duty to ensure that they have adequate intrusion detection systems so that they can timely

detect intrusions into their systems and networks and can take appropriate corrective action.

86. Additionally, Defendants owe a duty to confirm that any affiliates, vendors, or third parties whom Defendants are entrusting to manage, store, and secure the PII provided to Defendants by their customers have adequate security for that PII, follow industry standards and laws relating to safeguarding PII, have properly segregated that PII, have securely encrypted that PII, and otherwise prioritize data security in a way that will ensure the PII is secure from cyber threats and malicious actors.

87. Defendants owe a duty of care to Plaintiffs and members of the Class because they were and are foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and Class members and the critical importance of adequately securing such information.

88. Plaintiffs and members of the Class entrusted Defendants with their PII with the understanding that Defendants would safeguard their information. Defendants were in a position to protect

against the harm suffered by Plaintiffs and members of the Class as a result of the Data Breach whereas Plaintiffs and the Class members were dependent on Defendants for that protection.

89. Defendants' actions created a foreseeable risk of harm to Plaintiffs and Class members. Defendants' misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Data Breach, failing to properly encrypt the PII, failing to implement systems that could timely detect intrusions into their systems by threat actors, failing to train their personnel to recognize and respond to data security risks, or failing to ensure that parties entrusted by Defendants to store, manage, and secure the PII of Plaintiffs and the Class had those systems and procedures in place.

90. Defendants knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendants knew about – or should have been aware of - numerous, well-publicized data breaches affecting businesses that store PII in the United States.

91. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs' and Class members' PII. These duties are non-delegable.

92. Defendants breached their duties to Plaintiffs and Class members by failing to provide reasonable or adequate computer systems and data security to safeguard the PII of Plaintiffs and Class members.

93. Furthermore, Defendants negligently entrusted Plaintiffs' and the Class members' PII to third party vendors and service providers without taking adequate steps to ensure they had the systems and protocols in place to protect that PII from theft or disclosure.

94. Through Defendants' acts and omissions, including Defendants' failure to provide adequate security and its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members.

95. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to exfiltrate Plaintiffs' and Class members' PII and then misuse it, Defendants violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect Plaintiffs' and Class members' PII. Defendants also violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724, in that they disclosed the driver's license numbers of Plaintiffs and the Class members to unauthorized third parties.

96. Plaintiffs and the Class members are among the class of persons Section 5 of the FTC Act and the DPPA were designed to protect, and the injuries suffered by Plaintiffs and the Class members is the type of injury those laws were intended to prevent.

97. Neither Plaintiffs nor any of the Class members contributed to the Data Breach as described in this Complaint.

98. As a direct and proximate cause of Defendants' negligent conduct, Plaintiffs and Class members have suffered and/or will suffer injury and damages, including: (i) actual instances of identity

fraud or similar misuse of their PII; (ii) loss of their benefit of the bargain with Defendants; (iii) the publication, theft, or misuse of their PII, including instances of identity fraud or similar misconduct; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (viii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect that PII in its continued possession; and, (ix) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

COUNT 2

Unjust Enrichment

(On behalf of the Nationwide Class and all Subclasses)

(As to Defendants VWoA and Audi)

99. Plaintiffs incorporate by reference the allegations from paragraphs 1 through 82 as though fully set forth herein.

100. Plaintiffs bring this claim against Defendants VWoA and Audi on behalf of themselves, the National Class, and the Florida and California Subclasses.

101. Plaintiffs and members of the Class directly or indirectly conferred a monetary benefit on Defendants. Specifically, Plaintiffs and Class members paid for products or services of the Defendants and also provided and entrusted their PII to those Defendants, which Defendants used for sales and marketing purposes.

102. In exchange, Plaintiffs and Class members should have received from Defendants their expected goods and services, such as the security of their PII, and should have been entitled to have Defendants protect their PII with adequate data security, and timely notice of the Data Breach.

103. Defendants appreciated, accepted, and retained the benefit bestowed on them under inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiffs and Class members as described herein; Plaintiffs and Class members conferred a benefit on Defendants, and Defendants accepted or retained that benefit. Defendants profited from the products and services Plaintiffs and Class members paid for and used Plaintiffs' and Class members' PII for business purposes.

104. Defendants failed to secure Plaintiffs' and Class members' PII and therefore, did not provide full compensation for the monetary benefit Plaintiffs and Class members conferred on Defendants.

105. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

106. Had Plaintiffs and Class members known that Defendants would not secure their PII using adequate security, they would not have chosen to use Defendants' products or services, or would have paid less for them, and would not have entrusted their PII to Defendants.

107. Plaintiffs and Class members have no adequate remedy at law.

108. Under these circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

109. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money or items of value belonging to Plaintiffs and Class.

COUNT 3

Breach of Confidence

(On behalf of the Nationwide Class and all Subclasses)

(As to Defendants VWoA and Audi)

110. Plaintiffs incorporate by reference the allegations from paragraphs 1 through 82 as though fully set forth herein.

111. Plaintiffs bring this claim against Defendants VWoA and Audi on behalf of themselves, the National Class, and the Florida and California Subclasses.

112. At all times during Plaintiffs' and Class members' interactions with Defendants, Defendants were fully aware of the

confidential and sensitive nature of Plaintiffs' and Class members' PII that Plaintiffs and Class members provided to Defendant.

113. Defendants' relationship with Plaintiffs and Class members was governed by terms and expectations that Plaintiffs' and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

114. Plaintiffs and Class members provided their PII to Defendants with the explicit and implicit understanding that Defendants would protect and not permit the PII to be disseminated to any unauthorized parties.

115. Defendants voluntarily received in confidence Plaintiffs' and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

116. Due to Defendants' failure to prevent, detect, and avoid the Data Breach by following best information security practices to secure Plaintiffs' and Class members' PII, Plaintiffs' and Class Members' PII was disclosed to and misappropriated by unauthorized

third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

117. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and Class members have suffered the damages alleged.

118. But for Defendants' disclosure of Plaintiffs' and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and misused by unauthorized third parties. Defendants' disclosure through the Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

119. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class Members' PII. Defendants knew their systems and technologies for accepting and securing Plaintiffs' and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiffs' and Class members' PII in jeopardy.

120. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

COUNT 4

Breach of Implied Contract

(On behalf of the Nationwide Class and all Subclasses)

(As to Defendants VWoA and Audi)

121. Plaintiffs incorporate by reference Paragraphs 1 through 82 as though fully set forth herein.

122. Plaintiffs bring this claim against Defendants VWoA and Audi on behalf of themselves, the National Class, and the Florida and California Subclasses.

123. Defendants VWoA and Audi provided automobile products and services to Plaintiffs and Class members in exchange for compensation and other benefits. In so doing, Defendants either required Plaintiffs and Class members to provide their PII or acquired their PII with the authorization of Plaintiffs and the Class.

124. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiffs and Class members in their possession was only used to provide the agreed-upon services and other benefits from Defendants.

125. Defendants were therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure or use.

126. Plaintiffs and Class members accepted Defendants' offers for products and services and fully performed their obligations under the implied contract with Defendants by providing their PII, directly or indirectly, to Defendants.

127. Plaintiffs and Class members would not have provided and entrusted their PII to Defendants in the absence of their implied contracts with Defendants, and would have instead retained the opportunity to control their PII for uses other than products and services from Defendants.

128. Defendants breached their implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII.

129. As a proximate and direct result of Defendants' breaches of its implied contracts with Plaintiffs and Class members, Plaintiffs and the Class members suffered economic damages as described in detail above.

COUNT 5

Declaratory and Injunctive Relief

(On behalf of the Nationwide Class and all Subclasses)

(As to all Defendants)

130. Plaintiffs incorporate by reference the allegations from paragraphs 1 through 82 as though fully set forth herein.

131. Plaintiffs bring this claim against Defendants VWoA and Audi on behalf of themselves, the National Class, and the Florida and California Subclasses.

132. As previously alleged, Defendants owe duties of care to Plaintiffs and Class members that require Defendants to adequately secure the PII entrusted to them.

133. Defendants still possesses the PII pertaining to Plaintiffs and the Class members.

134. Defendants have made no announcement or notification that they have remedied the vulnerabilities in their practices and policies about ensuring the data security of Plaintiffs' and the Class members' PII.

135. Accordingly, Defendants have not satisfied their legal obligations and duties to Plaintiffs and the Class members. On the contrary, now that Defendants' lax approach towards data security has become public, the PII in their possession is more vulnerable than it was prior to announcement of the Data Breach.

136. Actual harm has arisen in the wake of the Data Breach regarding Defendants' obligations and duties of care to provide data security measures to Plaintiffs and the Class members, including the fact that Class members' PII is potentially available for sale on the dark web.

137. Plaintiffs therefore seek a declaration that Defendants' existing data security measures do not comply with their obligations and duties of care, and to comply with their obligations and duties of care, Defendant must implement and maintain reasonable security measures, including those set forth in the prayer below.

COUNT 6

Breach of Contracts to which Plaintiffs and the Class are third party beneficiaries

(On behalf of the Nationwide Class and all Subclasses)

(as against Defendant Shift Digital)

138. Plaintiffs incorporate by reference all allegations in paragraphs 1 through 82 as though fully set forth herein.

139. Plaintiffs bring this claim against Defendant Shift Digital on behalf of themselves, the National Class, and the Florida and California Subclasses.

140. At all times relevant, Defendant Shift Digital had express or implied contracts or agreements with several automobile manufacturers and dealers, including Defendants VWoA and Audi, to provide secure data and records management, retention, retrieval, and storage for marketing purposes.

141. Plaintiffs and the members of the Class are intended third-party beneficiaries of contracts entered into between Defendant Shift Digital and these manufacturers, dealers, and other business entities because their PII is a subject of the contracts and Defendant Shift Digital agreed to keep it secure as a part of providing data and records management, retention, retrieval, and storage to its customers.

142. Defendant Shift Digital breached these contracts by failing to provide secure or adequate data storage services, resulting in the

Data Breach and the theft and misuse of the PII of Plaintiffs and the Class by unauthorized third persons.

143. Plaintiffs and the members of the Class have a right to recovery for the breach because one or more of the parties to these contracts intended to give Plaintiffs and the Class members the benefit of the performance promised in the contracts.

144. As a direct and proximate result of Defendant Shift Digital's breaches of these contracts, Plaintiffs and the Class members suffered the injuries as described in detail above.

COUNT 7

Violation of the DPPA, 18 U.S.C. § 2724

(On behalf of the Nationwide Class and all Subclasses)

(As to all Defendants)

145. Plaintiffs incorporate by reference paragraphs 1 through 82 as though fully set forth herein.

146. Plaintiffs bring this claim against Defendants VWoA, Audi, and Shift Digital on behalf of themselves, the National Class, and the Florida and California Subclasses.

147. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

148. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(a). Drivers' license numbers are motor vehicle records under the DPPA.

149. Defendants obtain motor vehicle records from their customers.

150. Defendants also obtain motor vehicle records directly from companies and entities that provide such records.

151. From 2019 through 2021, PII of Plaintiffs and the Class, including their driver's license numbers were left unsecured and publicly available on Defendants' systems. Defendants thus knowingly both used and disclosed Plaintiffs' and Class members' motor vehicle records for a purpose not permitted by the DPPA pursuant to 18 U.S.C. §§ 2724 and 2721(b).

152. Through the Data Breach, Defendants disclosed motor vehicle records for purposes not authorized by the DPPA.

153. Plaintiffs and putative Class members are entitled to actual damages, liquidated damages, and attorneys' fees and costs.

COUNT 8

Violation of California's Consumer Privacy Act,

Cal. Civ. Code § 1798.150

(On behalf of the California Subclass only)

(As to all Defendants)

154. Plaintiff Villalobos incorporates by reference paragraphs 1 through 82 as though fully set forth herein.

155. Plaintiff Villalobos brings this claim against Defendants VWoA, Audi, and Shift Digital on behalf of himself and the California Subclass.

156. Defendants are corporations organized for the profit or financial benefit of their owners and have annual gross revenues exceeding $25 million and collect PII as defined in Cal. Civ. Code § 1798.140. In addition, Defendants annually buy, receive, sell, or share for commercial purposes the PII of more than 50,000 consumers.

157. Defendants violated section 1798.150(a) of the California Consumer Privacy Act by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Villalobos and the California Subclass. As a direct and legal result, Plaintiff's and the California Subclass's PII was subject to unauthorized access and exfiltration, theft, or disclosure.

158. As a direct and proximate result of Defendant's acts, Plaintiff Villalobos and the Class members were injured and lost money or property, including the loss of benefit of the bargain, the loss of their legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

159. Plaintiff Villalobos and Class members seek relief under section 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs.

160. On or about June 28, 2021, Plaintiff Villalobos sent Defendants VWoA and Audi via certified mail the 30-day notice letter as required under Civil Code section 1798.150, subd. (b). Because

Defendants VWoA and Audi have not cured, and cannot cure, the results of their violations of the CCPA, Plaintiff and the Class members seek statutory damages against these Defendants under Civil Code section 1798.150, subd. (b).

161. On or about August 6, 2021, Plaintiff Villalobos sent Defendant Shift Digital via certified mail the 30-day notice letter as required under Civil Code section 1798.150, subd. (b). Plaintiff and the Class members reserve the right to amend this Complaint as of right to seek statutory damages against Shift Digital and relief following the expiration of the 30-day period.

COUNT 9

Violation of Florida's Deceptive and Unfair Trade Practices Act,

Fla. Stat. § 501.201, et seq.

(On behalf of the Florida Subclass only)

(As to Defendants VWoA and Audi)

162. Plaintiff Adams incorporates by reference paragraphs 1 through 82 as though fully set forth herein.

163. Plaintiff Adams brings this claim against Defendants VWoA and Audi on behalf of himself and the Florida Subclass.

164. Defendants VWoA and Audi advertised, offered, or sold goods or services in Florida and engaged in commerce affecting Florida residents, including Florida Plaintiffs and members of the Florida Subclass.

165. Plaintiff Adams and the members of the Florida Subclass are consumers as defined in the FDUTPA, Fla. Stat. § 501.203.

166. Defendants VWoA and Audi engaged in unfair, unconscionable, and deceptive acts and practices in violation of the FDUTPA, Fla. Stat. § 501.203, including: (1) Failing to identify foreseeable risks to the security and privacy of the Plaintiff Adams' and Florida Subclass's PII, failure to fix or correct the identified security and privacy risks, failing to bring its data security and privacy practices up to industry standards or the standards required by law despite the known threats to the security of PII; (2) failing to implement reasonable security measures to protect the PII of Plaintiff Adams and members of the Florida Subclass; (3) failing to comply with industry standards for data security and failing to meet the requirements and duties for data security established by law, including those set forth in the FTC Act and Florida's data security

statute, Fla. Stat. § 501.171(2); deceptively representing, either through affirmative misrepresentation or omission, that VWoA and Audi would comply with industry standards and legal duties relating to data security and retention even though VWoA and Audi did not comply with such measures and duties, including those identified above, and did not adequately secure the Plaintiff Adams' and the Florida Subclass members' PII.

167. VWoA's and Audi's misrepresentations and omissions were material because they were reasonably likely to deceive reasonable consumers about the adequacy of VWoA's and Audi's data security measures and compliance with laws and standards relating to that data security.

168. Plaintiff Adams and members of the Florida Subclass acted reasonably in relying on the misrepresentations and omissions of Defendants VWoA and Audi and could not reasonably have uncovered the falsity of those misrepresentations and omissions.

169. The above-listed unfair, unconscionable, and deceptive acts and practices in violation of the FDUTPA were the direct and proximate cause of the Data Breach and the injuries suffered by the

Plaintiff Adams and members of the Florida Subclass, as detailed previously.

170. Had VWoA and Audi disclosed to the Plaintiff Adams and members of the Florida Subclass that their PII would not be kept secure and would be subject to theft, the Plaintiff Adams and members of the Florida Subclass would not have provided their PII to VWoA and Audi.

171. Plaintiff Adams and the Florida Subclass seek all monetary and equitable relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.211, declaratory and injunctive relief, attorneys' fees and costs pursuant to Fla. Stat. § 501.2105(1), and any other relief available under the FUDTPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;

c. Finding that Defendants engaged in the unlawful conduct as

alleged herein;

d. Enjoining Defendants' conduct and requiring Defendants to implement proper data security policies and practices; specifically:

   i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

   iii. requiring Defendants to delete, destroy, and purge the PII of Plaintiffs and the Class members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class members;

   iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the

Plaintiffs' and the Class members' PII;

v. prohibiting Defendants from maintaining Plaintiffs' and the Class members' PII on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised,

hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and the Class members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PII;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2

Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendants to design, maintain, and test their computer systems to ensure that PII in their possession is adequately secured and protected;

xix. requiring Defendants to disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendants to implement multi-factor authentication requirements;

xxi. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class members.

e. Awarding Plaintiffs and Class members damages, including

statutory damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Dated: August 9, 2021

WILSON & BROWN, PLLC

/s/ Karen N. Wilson-Robinson
Karen N. Wilson-Robinson
2066 Central Park Avenue
Yonkers, New York 10710
Telephone: (646) 498-9816
Facsimile: (718) 425-0573
karen@wilsonbrownlawyers.com

Gayle M. Blatt, *pro hac vice application forthcoming*
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, California 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com